Symantec Services

State of Iowa

September 29, 2005

Agenda

- Recap of the Iowa Department of Human Services Managed Security Services Pilot
  - What are Managed Security Services?
  - What did Symantec monitor during the pilot?
  - Key findings during the pilot
  - Value to the State
- Recap of Assessment with Iowa Judicial
- Symantec's Involvement with State Initiatives Across the Country

What is Symantec's Managed and Monitored Security Service?

- Two Service Components offered through Symantec's Secure Operations Center (SOC)
  - Monitoring
    - The correlation of logs across disparate devices.
    - Detailed analysis and queries against data to give detailed events generation across the entire organization
    - Actionable remediation information escalated to appropriate client contacts

      Benefit: Allows organizations to focus on maintaining their networks and remediating issues via focused 24X7 security expertise and technology
  - Management
    - Health and feeding of the device
    - Secure policy creation
    - Audit tracking of changes to the device

      Benefit: Alleviates the menial tasks of maintaining network devices and tracking changes to the device

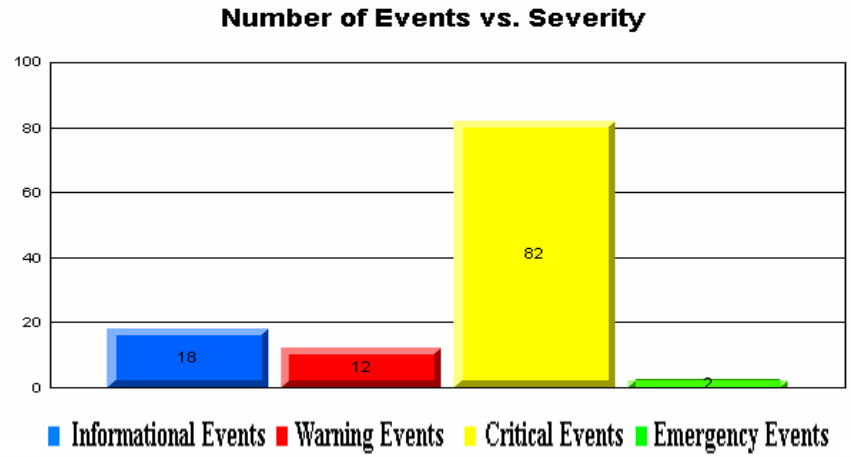
Why is this Important to the State

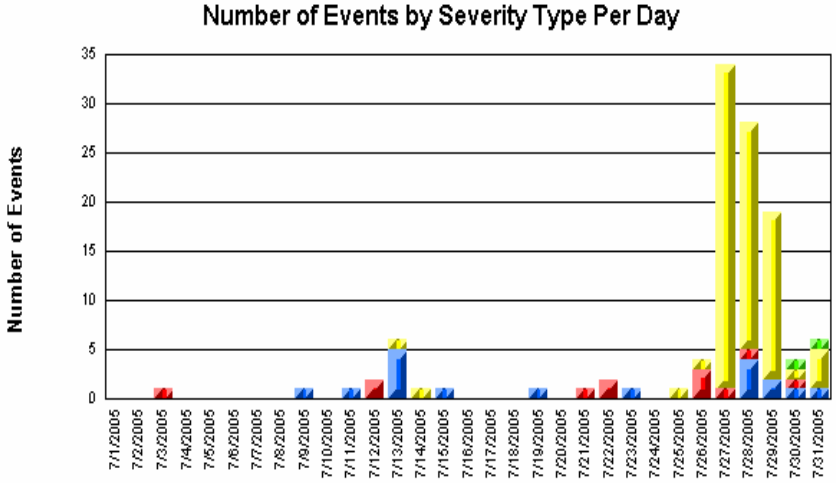
- States are challenged with attracting and retaining a high level of security expertise. The expertise that is in place at the State should be used for pro-active security management. By utilizing an MSS service the State receives:
  - 24 x 7 monitoring (equivalent to 5 FTE's)
  - Top Level Security Advisors providing actionable advise
  - The off-loading of time consuming log consolidation and analysis to "technology"
- MSS Provides Regulatory Compliancy
  - Log monitoring is required control under Sarb-Ox, HIPAA, others
- Early Warning/Global Insight allows a reduction in "reactionary" events – placing the State in a much more pro-active security stance

Symantec MSS offering for Iowa DHS

- 60 Day Pilot to test drive the service included:
  - Firewall Monitoring of one firewall
  - Intrusion Detection Systems (IDS) Management & Monitoring of one IDS device
- The devices being monitored were located within the Iowa DHS Network (only monitoring DHS network traffic, not other State network traffic)

Summary of Events for the Month of July





Security event summary

Number of logs imported 7,993,198
Number of sub-events generated 41,296
Number of events generated 4,141
Number of events commented 114
Number of Informational events 18
Number of Warning events 12
Number of Critical events 82
Number of Emergency events 2

Key Benefits to DHS during the 60 day Pilot

- Two major Worm Outbreaks
  - Symantec identified these attacks immediately (one on a Sunday night, the second on a Saturday morning)
  - Identified infected systems and outlined containment initiatives and communicated this to appropriate DHS personnel

    Value to the State

    - *24 hour notification for early detection*
    - *Detailed description of steps to be taken by the State*
    - *Pinpointed systems that had the worm and needed repair*
- Severe incident warning of heavy port scanning from inside the network against a SQL database. With this information, DHS was able to identify that it was an internal developer within an hour.

  Value to the State

  - *Real-time notification of abnormal database scans. SQL injection is a very common, yet serious application vulnerability exploit – if it had been a malicious attack, would have been quickly contained*

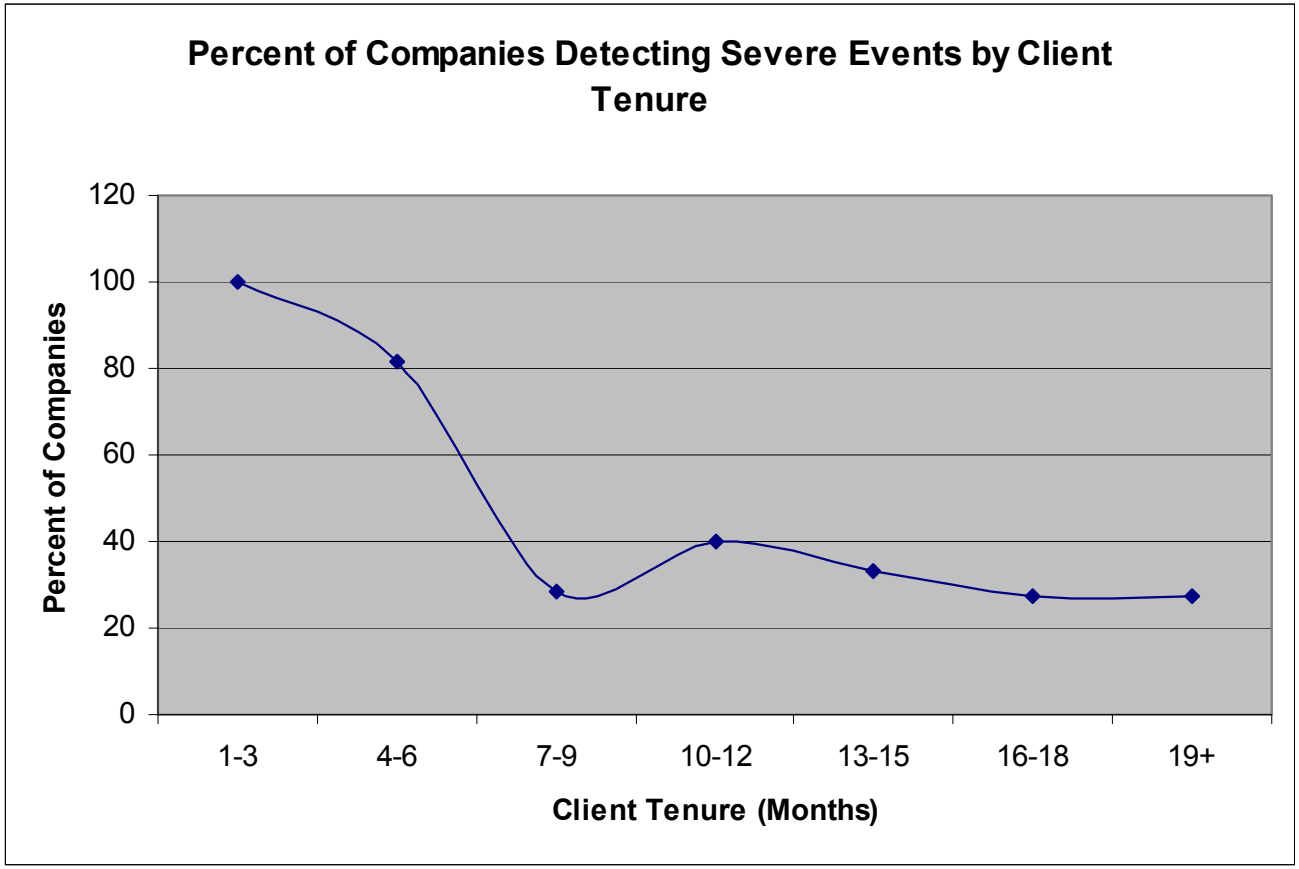
Findings during the 60 day Pilot

- On top of severe incidents, there were many informational warning events that occurred, giving DHS deeper insight into the types of attacks going on across the network.

  Value to the State

  - *Immediate alerting on suspicious activity.*
  - *Almost 8 million logs were generated from the two devices over the first 30 day window. This correlated to 114 events that were commented on by the SOC, with 12 warning events and 82 critical events*
  - *Broader knowledge of network activity*
  - *Long term, a more stable and secure network resulting in fewer severe incidents*

Net Result: Clients are Compromised Less Over Time



Symantec Security Advisory Services

Secure Application Services

- Application Penetration Testing
- Application Architecture Assessment
- Commercial Product Assessment
- Application Security Principles Training
- Secure Code Reviews
- Secure Application Development Services

Strategy Services

- Security Strategy Development
- Security Program Evaluation
- Security Program Development & Support
- Vendor & 3rd Party Risk Assessment

Compliance Services

- Regulatory & Standards Compliance Assessments
- PCI Assessments
- ISO 17799 Gap Assessment

Secure Infrastructure

- Network Architecture Assessment & Design Review
- Network Penetration Assessment
- Network Vulnerability Assessment
- Wireless Security Assessment
- Host Vulnerability Assessment
- Infrastructure Security Principles Training
- Host Hardening & Secure Build

Operations Services

- Security Policy Assessment
- Incident Management Design & Staffing
- Cyber Attacks & Countermeasures
- Security Awareness Program Development

Assessment with Iowa Judicial

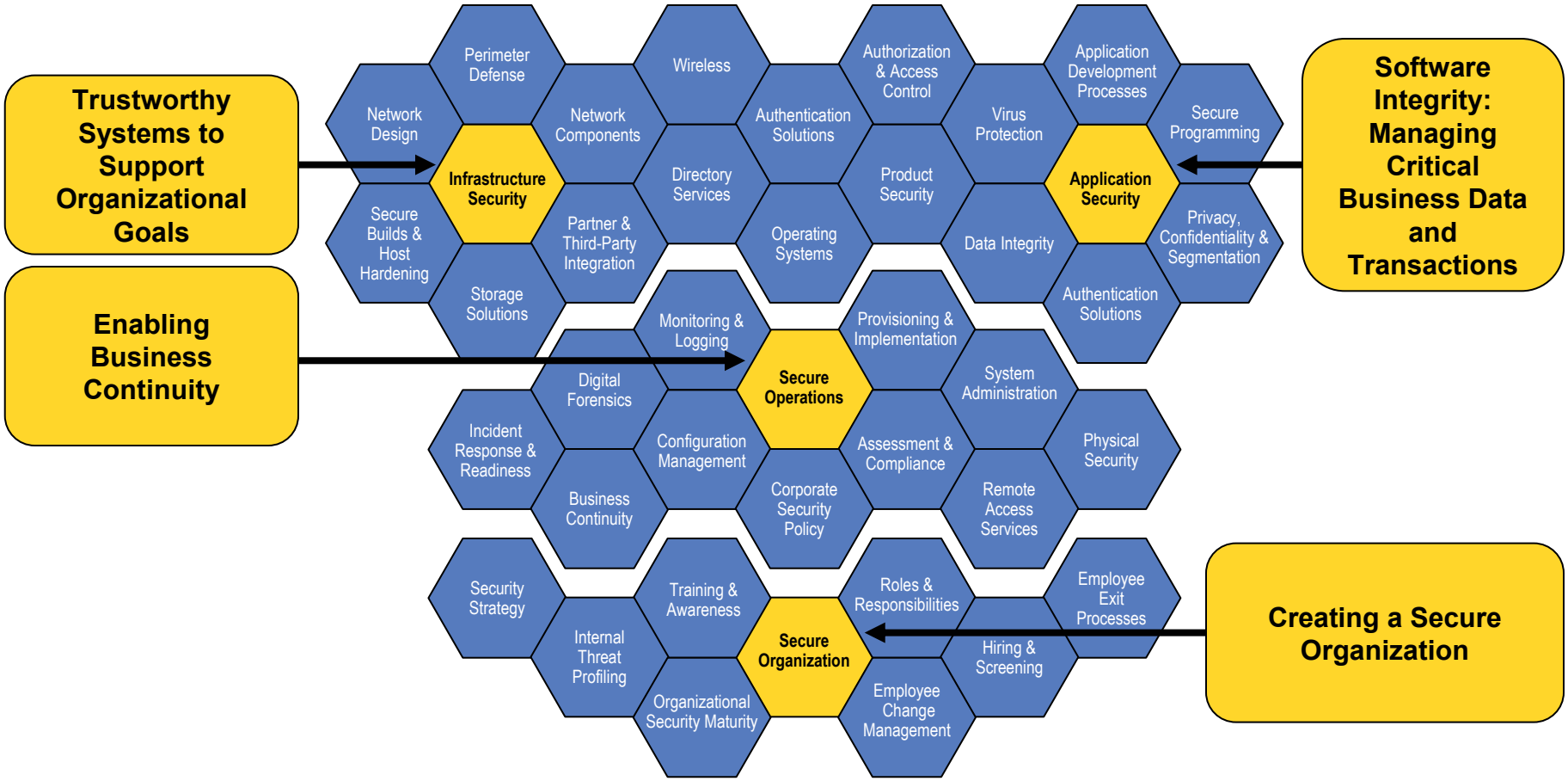
Work Conducted:

- Network Vulnerability Assessment
  - Review network security reviewing items such as:
    - Firewall configuration, wireless configuration, and virtual private networks (“VPN”) for vulnerabilities or insecure configuration
  - Assess representative host operating system configurations including:
    - UNIX AIX Server
    - Linux Server
    - Windows NT/2000/2003 Server
    - Oracle Database Server
- Network Penetration Test
- Report on Assessment

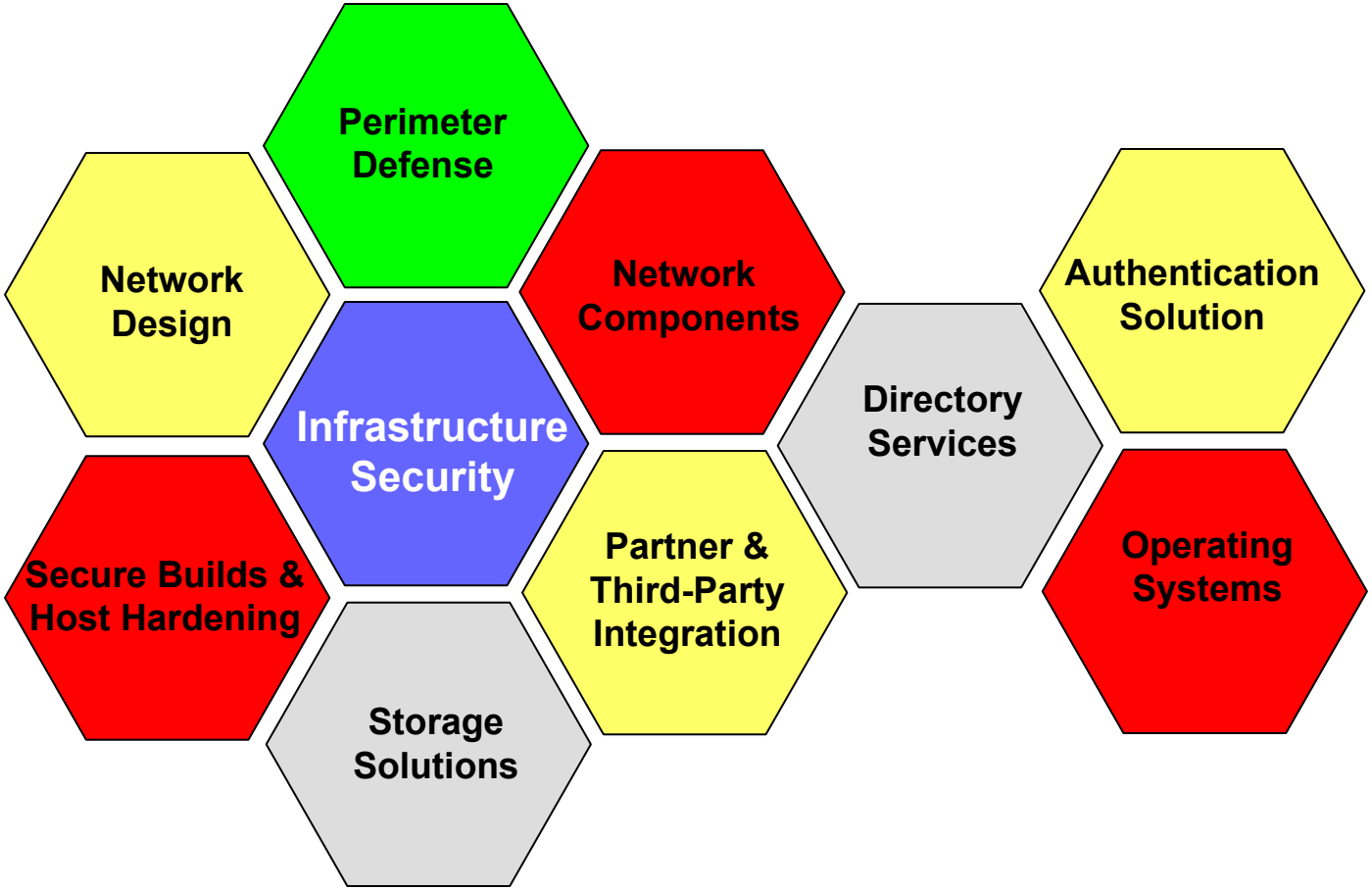
Assessment with Iowa Judicial

- Methodology Used
- Results
- Recommended Next Steps

Symantec Security Blueprint



Security Blueprint - Infrastructure



Areas not assessed or touched upon during this engagement

Areas that do not meet industry standards and pose a high risk

Areas that could be improved and represent a smaller risk than red

Areas that meet or exceed industry standards and risk is effectively managed

What are other States doing with Symantec?

- Using Symantec Managed Security Services
  - Oregon
  - New York (Building their own SOC with Symantec personnel and technology)
- Using Symantec for Security Assessments (including Iowa)
- Using Symantec's DeepSight Alerting Services
- Enacting Anti-Spam legislation and utilizing Symantec technology and consulting to enforce
- Implementing Symantec products such as: Network Appliances, Anti-Virus, Anti-Spam, Enterprise Administration products,
- Conducting "Inform" Workshops to quantify security investments

Thank You!